LAW OFFICES OF
GERALD B. LEFCOURT, P.C.
A PROFESSIONAL CORPORATION
1776 BROADWAY, SUITE 2000
NEW YORK, N.Y. 10019

GERALD B. LEFCOURT
lefcourt@lefcourtlaw.com

TELEPHONE
(212) 737-0400
FACSIMILE
(212) 988-6192

SHERYL E. REICH
reich@lefcourtlaw.com
FAITH A. FRIEDMAN
ffriedman@lefcourtlaw.com

January 9, 2020

VIA ECF

The Honorable J. Paul Oetken
United States District Judge
Southern District of New York
United States Courthouse
40 Foley Square
New York, NY 10007

United States v. Kukushkin, et al. 19 CR. 725 (JPO)

Dear Judge Oetken:

We are counsel for Andrey Kukushkin, a defendant in the above referenced matter. We write on behalf of the defense in response to the government's January 3, 2020 letter opposition and in further support of the defense's December 12, 2019 application pursuant to 18 U.S.C. § 3504 (Dkt. No. 45).

Yet again, the government's submission raises more questions than it answers and provides further support for the defendants' application. Indeed, the government has all but admitted the existence of FISA materials and other electronic surveillance, none of which it intends to turn over. The gravamen of the government's contention is that since "it does not intend to use any information obtained or derived from FISA or other forms of surveillance", it is not required to make any disclosures. The government's insistence that it is not using such evidence should not end this Court's inquiry; rather, it should ***begin*** the inquiry.

Having established a colorable basis for its claim, the defense's application should be granted.

The Government's Covert Surveillance of United States Citizens

As detailed in our opening letter, the government routinely and secretly surveilles and intercepts communications of United States citizens without judicial authorization or review. This surveillance goes well beyond that authorized under FISA and includes, *inter alia,* surveillance under the FISA Amendments Act (FAA), Executive Order (E.O.) 12333, and National Security Letters (NSLs). What's more, it is now widely known that the government regularly exploits surveillance directed at foreign persons as a tool against United States persons as to whom law enforcement is specifically prohibited from targeting. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Sec. 702*

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

of the of the Foreign Intelligence Surveillance Act, July 2 2014 (https://www.pclob.gov/library/702-Report.pdf) (the "PCLOB Report"). Chief among these exploitive tools are prolific queries of personal data collected under Section 702 of the FAA. *Id.* at p. 59 ("whenever the FBI opens a new national security investigation or assessment, … [it] will query previously acquired information from a variety of sources, including Section 702… FBI personnel will also query this data, …in …criminal investigations …unrelated to national security efforts".). *See also* https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf.[1] What's more, such searches are not limited to 702 surveillance databases. Ryan Gallagher, *The Surveillance Engine*, Intercept, Aug. 25, 2014, http://bit.ly/1A1VFLL. There is every reason to believe the same occurred here.

The majority of warrantless surveillance, however, is conducted outside the parameters of FISA, pursuant to E.O. 12333 or other purported authorities.[2] Although directed only to activities outside the United States conducted by foreign persons and governments, E.O. 12333 in fact permits the collection, retention, and dissemination of information concerning United States persons that is "incidentally obtained", if the information "may indicate involvement in activities that may have violated Federal, state, local, or foreign law". E.O. 12333, Part 2, §2.3(i). Law enforcement uses E.O. 12333 information when investigating individuals within the United States, including in the absence of national security threats or implications. *See Two Sets of Rules for Surveillance*, N.Y. Times, Aug. 13, 2014, http://nyti.ms/1u2juDt (chart describing uses of E.O. 12333 surveillance); Gallagher, *The Surveillance Engine, supra,* http://bit.ly/1A1VFLL.

As a result, the lines between domestic and foreign surveillance have blurred, if not completely disappeared. Under the auspices of E.O. 12333, United States agencies engage in bulk surveillance programs not subject to judicial or congressional oversight. *See* Dkt. No. 45 at pp. 2-3. Among them is the bulk seizure of financial data and phone records, including the contents and records of telephone calls, video chats, emails, internet activity and text messages,

---

[1] According to an opinion of the FISC, in 2017 alone, the FBI conducted more than 3.1 million warrantless queries of Section 702 databases, a "significant percentage" of which likely involved United States persons. *Id.* at p. 66. As the FISC observed, the privacy implications of these queries are "substantial" (*id.* at p. 88), still, the FBI's policy has been to encourage "maximal querying of Section 702 information", including at the earliest stages of domestic investigations. *Id.* at 72, 75.

[2] *See* NSA Legal Fact Sheet: Executive Order 12333 (June 19, 2013) ("FISA only regulates a subset of NSA's signals intelligence activities. NSA conducts the vast majority of its SIGINT [signal intelligence] activities solely pursuant to the authority provided by Executive Order (EO) 12333".).

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

of United States persons; the deployment of "stingrays" to track cell phones;[3] the secret implantation of malware on personal computers; and, sweeping internet surveillance – all without a warrant. The defense has specifically inquired about the government's use of many of these surveillance techniques. The government refuses to "affirm or deny" its existence, instead focusing its responses on "FISA" and "Title III" evidence.

To compound matters, the government has universally taken the position that it has no legal obligation to provide notice in criminal prosecutions when its evidence is the fruit of E.O. 12333 surveillance. Charlie Savage, *Reagan-Error Order on Surveillance Violates Rights, Says Departing Aide,* N.Y. Times, August 13, 2014. Thus, it is no surprise that in this case the government appears to be taking the same approach. Indeed, the government has remained eerily silent, failing even to mention E.O. 12333 in its opposition or deny use of E.O. 12333 surveillance in this investigation. Even worse, despite the deafening silence, the government has seemingly filed with this Court a secret submission justifying it. *See* Dkt. No. 61 at fn. 1.

But the government's efforts at concealment of these novel tools go well beyond contentions that it has no obligation to disclose. In fact, the government has engaged in the practice of "parallel construction", the process of using a non-controversial investigative technique to ***reobtain*** evidence originally obtained from a controversial one. *See also* Dkt. No. 45 at pp. 3-4. As if that were not enough, the government's fallback position, the one it sees as the surest way to avoid disclosure, is to make bald conclusory assertions that it does not intend to use any illegally obtained evidence or any evidence derived therefrom at trial. Of course, no one – not the Court, not the defendants, possibly not even the prosecutors assigned to this case – knows the basis for that conclusion. It is well-guarded secreted information.[4] Nor does it address whether such evidence ***already*** has been used. The government's January 3, 2020 opposition – with all its obfuscation and subterfuge – is more of the same.

Applicable Law

The Fourth Amendment provides Americans with a protected privacy interest in the contents of their communications, including telephone call, emails, text messages, and video

---

[3] Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, Wall St. J., Nov. 13, 2014, https://on.wsj.com/2L0nXWH; Devlin Barrett, *CIA Aided Program to Spy on U.S. Cellphones*, Wall St. J., March 10, 2015, https://on.wsj.com/30EUbw1.

[4] Within the Department of Justice there exists a 31-page Policy Memorandum dated November 2016 titled "Determining Whether Evidence is 'Derived From' Surveillance Under Title III or FISA". The memorandum includes a legal analysis of Title III, FISA, and relevant caselaw, focusing on the present state of the law as to when evidence is deemed to have been "derived from" electronic surveillance under these statutory frameworks. The Department of Justice has rebuffed all efforts at disclosure and refused to provide it in response to FOIA requests made by the ACLU. *See* Declaration of Susan L. Kim, Dkt. No. 25-1 in *ACLU v. United States Department of Justice,* 17-cv-3571 (JSW) (N.D.Cal.).

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

chats. *See United States v. U.S. Dist. Court*, 407 U.S. 297, 313 (1972). Illegally intercepted communications, *i.e.,* those obtained without a properly issued judicial warrant or pursuant to an exception to the warrant requirement, are not admissible in any proceeding against an accused; nor are the fruits that flow from that evidence. 18 U.S.C. § 2515; *Gelbard v. United States,* 408 U.S. 41, 46 (1972); *Wong Sun v. United States,* 371 U.S. 471, 486-88 (1963) (explaining "fruit of the poisonous tree" doctrine); *Murray v. United States,* 487 U.S. 533, 536-37 (1988) (as to right to seek suppression of evidence "derived" from an unlawful search). It is axiomatic that to be able to vindicate and protect their rights, defendants subject to surveillance must test – in an adversarial proceeding – whether the government's evidence is the direct product of or derived from illegal searches. *United States v. U.S. District Court, supra,* 407 U.S. 297; *Alderman v. United States*, 394 U.S. 165 (1969); *see also, Wong Sun v. United States,* 371 U.S. at 486-88; *Murray v. United States,* 487 U.S. at 536-37.

Before illegally obtained evidence or the fruits thereof can be suppressed, the existence of such evidence and the manner by which it was obtained must be ascertained. Without such notice, a defendant has no meaningful opportunity to seek suppression and a court has no mechanism to "provide the scrutiny which the Fourth Amendment exclusionary rule demands". *Alderman v. United States,* 394 U.S. at 184, 184-85; *see also, Berger v. New York,* 388 U.S. 41, 60 (1967). It is not for the government to unilaterally decide the relevance and legality of the evidence it gathered. Nor can it avoid disclosure with conclusory and self-serving assertions that evidence was obtained lawfully, that it was not derived from unlawfully obtained evidence or that the government does not intend to use it at trial. On the contrary, where warrantless surveillance exists, the government must "affirm or deny" its existence, "even if the government believes it was lawful". Kris & Wilson, 2 *National Security Investigations & Prosecutions* § 27:12 (2d ed. 2012); *see also* 18 U.S.C. § 3504.

Section 3504 was enacted to protect the rights of victims of illegal electronic surveillance by requiring notice of same. *See Hearings on S. 30 Before Subcomm. No. 5 of the House Comm. On the Judiciary,* 91st Cong., 2nd Sess. 84, 104 (1970); *see also Gelbard v. United States,* 408 U.S. at 56. Under the statute, if a party in a proceeding before any court[5] claims that "evidence is inadmissible" because "it is the primary product of an unlawful act or because it was obtained by the exploitation of any unlawful act" then the government must "affirm or deny the

[5] It is not limited to challenging "questions propounded … in adjudicatory proceedings", as the government suggests. Indeed, as the Department of Justice acknowledges, it can be used as a discovery device. Department of Justice Criminal Resource Manual ("CRM") at 35, Defendant Motion ***or Discovery Request*** for Disclosure of Defendant Overhearings and Attny Overhearings ("In response to a defendant's motion ***or discovery request*** alleging unlawful electronic surveillance of the defendant…") (emphasis supplied). Nor is it limited to "court or grand jury proceedings". It applies with equal force to trials, hearing, or other proceedings before any "department, officer, agency, regulatory body, or other authority of the United States". *See* 18 U.S.C. § 3504(a).

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

occurrence of the alleged unlawful act". *See* 18 U.S.C. § 3504. The statute defines "unlawful act" as "the use of any electronic, mechanical, or other device" in violation of the law. *Id.* § 3504(b).[6]

A claim under § 3504, requires more than "mere suspicion", however, all that is necessary to trigger the government's obligation to inquire and respond is the existence of a "colorable basis". *See United States v. Pacella,* 622 F.2d 640, 643 (2nd Cir. 1980); *accord* Department of Justice Criminal Resource Manual ("CRM") at 36. Responses are to be encouraged. *See United States v. James,* 609 F.2d 36, 42 fn. 22 (2d Cir. 1979) ("We need not determine whether it was necessary for the government to file a response, as it did… Such a response, even if not required, …***is to be encouraged***".) (emphasis supplied). According to the Department of Justice's internal guidelines, once the duty to inquire is established, the government's duty is as follows:

> Generally, the government has an obligation pursuant to the provisions of 18 U.S.C. § 3504, to conduct a search of the appropriate agencies and to affirm or deny a claim that a defendant has been illegally overheard. This search is initiated at the request of the United States Attorney, to the Policy and Statutory Enforcement Unit of the Office of Enforcement Operations of the Criminal Division, and the results of the check are reported to that office.

CRM at 36, Defendant Overhearings; *see also id.* at 35.

Discussion

The government's opposition can be summarized as follows: (1) it has complied with its disclosure obligations under § 1806 of FISA (Dkt. No. 61 at 2-3); (2) the defense's § 3504 motion is procedurally and substantively improper (*id.* at 3-4); and (3) it is aware of its discovery and *Brady* obligations and intends to fully comply (*id.* at 5). We address each in turn.

FISA

Initially, the government contends that the defense's application should be treated as one under § 1806 of FISA. The defense's request, however, was very specific and very clear:

> … pursuant to 18 U.S.C. § 3504, …the government [should] be required to (a) inquire of government agencies and "affirm or deny" whether the defendants' oral or wire communications, including written communications, have been intercepted by means ***other than Title III or FISA warrants***, including by means

[6] Title III, FISA, and FAA have notice requirements as well; however, these provisions apply only to surveillance conducted under those statutory schemes, while § 3504 applies more broadly.

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

> of Executive Order 12333 ("E.O. 12333") and other surveillance; and (b) if so, to identify such evidence and delineate all fruits thereof.

(Dkt. No. 45 at 1) (emphasis supplied) (footnote omitted). In other words, the defense's § 3504 application is not made under nor should it be considered under FISA.

To be sure, as the government so aptly points out (Dkt. No. 61 at fn 3), at the time of its December 12, 2019 submission, the defense believed that no FISA evidence was obtained by the government. That no longer appears to be the case. To the extent FISA surveillance of the defendants occurred, the Court should require the government to provide the defense with FISA notice and should further ascertain, through adversarial proceedings, as to the genesis of such evidence and the extent to which it was used during the course of the government's investigation. In addition, the Court should require the government to disclose whether it engaged in warrantless queries of data gathered pursuant to Section 702 of the FAA, and if so, ascertain the bases for and circumstances under which those queries occurred, as well as how the government used the fruits of those queries. *See United States v. Agron Hasbajrami*, Dkt No. 15-2684-L; 17-2669-CON.

Perhaps the government takes this position because it believes it will fare better under § 1806, when asserting it does not intend to "use any FISA-obtained or FISA-derived information against the defendants at trial". Dkt. No. 61 at 2. It does not. As we pointed out in our opening submission, even in the FISA context defendants are entitled to know whether the government overheard or intercepted their communications and whether other evidence was derived therefrom. *See United States v. Belfield*, 692 F.2d 141, 146 (D.C. Cir. 1982) (in FISA context "even when the Government has purported not to be offering any evidence obtained or derived from electronic surveillance, a criminal defendant may claim that he has been the victim of an illegal surveillance and seek discovery of the logs of the overhears to ensure that no fruits thereof are being used against him"); *see also See United States v. Agron Hasbajrami*, Dkt No. 15-2684-L; 17-2669-CON.

What's more, although quick to assert it does not intend to use FISA evidence or evidence derived therefrom at trial in this matter, the government makes no representations as to whether FISA derived evidence was used during the course of the grand jury investigation, including to establish probable cause for the search warrants issued in this case, as a basis to seek subpoenas, or whether such evidence was admitted before the grand jury. Again, the Fourth and Fifth Amendments demand that the defendants be provided with this information.

18 U.S.C. § 3504

As relates to § 3504, the government argues that the defendants' request is premature (procedurally improper) and without a "colorable basis" (substantively improper). As to the former, without authority or further explanation, the government claims § 3504 is only available

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

"for a witness or defendant to challenge evidence when it is introduced". Dkt. No. 61 at 3. While it is often the case that a § 3504 application is made at or about the time the government seeks to admit certain evidence as to which the claimant was unaware and contends was unlawfully obtained, no such requirement is contained within § 3504. Indeed, the government's position is belied by its own internal guidelines. CRM at 35 ("In response to a defendant's motion or ***discovery request*** alleging unlawful electronic surveillance of the defendant…Elsur requests should be made ***at the earliest opportunity*** in order to give the agencies involved sufficient time to conduct a thorough and accurate search") (emphasis supplied); Stephen L. Harwood, Senior Counsel, *Electronic Surveillance Issues*, Office of Enforcement Operations, Criminal Division, Department of Justice, November 2005, at 129, *citing, U.S. v. Yaganita,* 552 F.2d 940, 944 (2d Cir. 1977) (motion made on opening day of trial untimely) https://www.justice.gov/sites/default/files/criminal/legacy/2010/04/11/elec-srvlnce-issuse.pdf.

Nor would such a requirement make sense. An agency search pursuant to § 3504 could take as many as 6 to 8 weeks. *See* CRM at 35. Is the government really suggesting that a witness or defendant must wait to make a § 3504 motion and thereby delay a grand jury presentation, hearing, trial, or other proceeding for weeks? Essentially, it is of no moment whether a trial date or hearing has been set in this matter. Legal proceedings in this criminal prosecution are ongoing and by the express terms of § 3504, the defendants' application is ripe.

Even if procedurally proper, it is the government's position that the defense has failed to establish a "colorable basis" for its claim and thus the application is substantively improper and should be denied. Dkt. No. 61 at 3. The government is wrong.

Section 3504 is intended to be invoked by those defendants like the defendants herein, who lack the proof necessary to demonstrate their communications were illegally intercepted but have a "colorable basis" for their claim. Because surreptitious electronic surveillance is by its nature covert, the facts available to defendants at this stage are necessarily limited. Courts applying § 3504 have recognized this reality, and what the defense has presented here is more than enough. *See e.g. United States v. DiLorenzo*, 1995 U.S. Dist. LEXIS 4539 (AGS) (S.D.N.Y. April 7, 1995) (existence of consensual recordings between defendant and informants enough to establish colorable basis under § 3504); *United States v. Staple,* 1979 U.S. Dist. LEXIS 9646 (S.D.N.Y. Sept. 21, 1979) (existence of mechanical difficulties with a telephone coupled with prior wiretapping of co-defendant by Canadian authorities years earlier constitutes colorable basis).

The defense's claim is anything but "speculative" and is based on more than "suspicion" and the involvement of "foreign nationals, foreign government officials, foreign communications [and] foreign travel" – all of which are present to a degree and kind that takes this case "outside the norm for criminal case in this District". Dkt. No. 61 at 4. Among the many facts supporting their claim is the following:

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

- the alleged existence of foreign communications between certain of the defendants and high-ranking Ukrainian government officials concerning the removal of the former United States Ambassador to the Ukraine;
- the purported existence of foreign communications between certain of the defendants and high-ranking United States government officials concerning the removal of the former United States Ambassador to the Ukraine, in part at the request of high-ranking Ukrainian government officials;
- supposed contributions to Republican linked political committees, including those connected ***to the President***, as well as campaigns of other high-ranking politicians and political candidates, by foreign nationals, including Russians, in contravention of federal election laws;
- alleged travel (and communications) overseas, including within Russia, during the course of the purported conspiracies, the details of which the government is keenly aware and has cited;
- supposed communications between Mr. Parnas and an indicted Ukrainian billionaire being sought by the United States for extradition to the United States from Vienna which the government is keenly aware and has cited;
- allegations of matters of national security, as evidenced by the congressional impeachment inquiry, the subsequent congressional reports (in which Mr. Parnas is identified by name), and media reports. Indeed, Mr. Parnas has been subpoenaed by the House for information related to this case as part of its impeachment proceedings;
- the apparent existence of FISA surveillance; and
- the involvement of United States intelligence officers and agencies.

The government does not deny a single factual contention made by the defense. Nor do these facts exist in a vacuum. We submit they must be considered in the context of the extensive surveillance of foreign and United States persons that is undertaken daily by the government, in particular, law enforcement queries of warrantless interceptions as a matter of course when criminal investigations are initiated.

Still, most telling of all is the government's own statements. Initially, it was the government's repeated insistence that "no Title III warrants were used in this investigation", even when asked whether non-Title III surveillance occurred. This was coupled by the government's refusal to answer direct and repeated questions as to its use of stingray and other electronic surveillance. Indeed, other than Title III warrants, there is not a single form of surveillance that the government has denied using in the course of this investigation, which

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

makes sense and proves the defense's point. The government also refused to submit an inquiry request to the Department of Justice and insists this inquiry is governed by FISA, not § 3504. Finally, but most telling of all, is the government's opposition. Not only does the government, for the first time, all but admit FISA warrants were obtained during the course of this investigation (*see* Dkt. No. 61 at fn. 3) but it felt compelled to make a confidential, sealed, *ex parte, in camera* submission to justify non-disclosure (*id.* at fn. 1). Not a single case cited by the government is on all fours.

The defendants have made more than a colorable claim that they have been subjected to warrantless and unlawful electronic surveillance by the government and their application should be granted.

Rule 16 Discovery and *Brady*

Finally, the government contends that it is aware of and intends to comply with its discovery and *Brady* obligations although it does not intend to produce classified discovery or make a CIPA motion. *See* Dkt. No. 61 at 5. Reliance upon the government's representations in this regard, without requiring it to provide at a minimum notice as to whether the subject surveillance occurred is fraught. To be sure, the results of an investigation by Department of Justice's own Office of the Inspector General leads one to question the propriety of such an approach. *See* DOJ OIG Annex to the Report on the President's Surveillance Program, July 10, 2009, at 35 ("We found that the Department made little effort to understand and comply with its discovery obligations … We believe that the Department should consider whether it must re-examine past cases to see whether potentially discoverable but undisclosed Rule 16 or *Brady* material was collected by the NSA…") https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-III.pdf).

Unquestionably, any of requested surveillance would fall squarely within Rule 16 discovery (*see* Rules 16(a)(1)(E)(i) and 16 (a)(1)(B)(i)), and is likely to be a fruitful source of *Brady* material. Indeed, Department of Justice guidelines acknowledge as much. CRM at 2052 (stating prosecutors are "compelled" to contact the intelligence community (IC) regarding criminal investigations and "must search" the IC files "if the prosecutor has actual or implied knowledge that the IC files contain Rule 16, Jenks, *Brady*, or Section 3504 materials).

Conclusion

The government's insistence on complete secrecy is incompatible with the rights of defendants, particularly in the face of rapidly advancing technology. Indeed, the Supreme Court's recent decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (prohibiting warrantless collection of cell-site location information), and the Second Circuit's decisions in *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (prohibiting bulk collection of phone records), and *United States v. Agron Hasbajrami*, Dkt No. 15-2684-L; 17-2669-CON (vacating

LAW OFFICES OF
GERALD B. LEFCOURT, P.C.

conditional plea and remanding to district court for examination and determination as to whether law enforcement queries of the product of warrantless electronic surveillance reasonable within the meaning of the Fourth Amendment), show why judicial oversight is essential to protecting individual liberty.

In the context of this case, with these facts, and in the face of the government's responses and silence, and the surveillance activities that are conducted daily by the intelligence community and law enforcement, it is inconceivable that there were no warrantless interceptions of defendants' oral and written communications. The government has all but admitted it.

Having established a "colorable basis" sufficient to trigger the government's inquiry obligations, the government should be ordered to undertake a comprehensive "agency search" and "affirm or deny" the existence of this evidence. The defendants are entitled to know the extent of the government's surveillance, and to litigate—in an adversarial proceeding—whether any of the government's evidence was derived from it. We respectfully submit that to find otherwise would render § 3504 meaningless.

We thank the Court for its consideration.

Respectfully submitted,

Gerald B. Lefcourt

cc: All counsel (via ecf)